PCT/GB2004/002754

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ



I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

I also certify that the application is now proceeding in the name as identified herein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



Signed

Dated 8 July 2004

GB 0315886.2

By virtue of a direction given under Section 30 of the Patents Act 1977, the application is proceeding in the name of:

STEM VENTURES LIMITED,
90 Fetter Lane,
LONDON,
EC4A 1JP,
United Kingdom

Incorporated in the United Kingdom,

[ADP No. 08888125001]

Patents Form 1/77

Patents Act 1977
(Rule 16)

THE PATENT OFFICE
- 7 JUL 2003
LONDON

The Patent Office

1/77

08JUL03 E820497-1 D02029
P01/7700 0.00-0315886.2

# Request for grant of a patent

*(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)*

The Patent Office

Cardiff Road
Newport
Gwent NP10 8QQ

1. Your reference — J00045637GB

2. Patent application number
*(The Patent Office will fill in this part)* — 0315886.2 — - 7 JUL 2003

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

WAY, Benjamin Bernard Peter
Flat 2
231 Sussex Gardens
London
WC2 2RL
United Kingdom

SECTION 30 (1)(b) PCT ACT) APPLICATION FILED 10/5/04

Patents ADP number *(if you know it)*

If the applicant is a corporate body, give the country/state of its incorporation — GB

8668592001

4. Title of the invention — Anti-Piracy System

5. Name of your agent *(if you have one)* — RGC Jenkins & Co.

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

26 Caxton Street
London SW1H ORJ
United Kingdom

Patents ADP number *(if you know it)* — 03966736001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications *(and if you know it)* the or each application number

| Country | Priority application number *(if you know it)* | Date of filing *(day / month/ year)* |
|---|---|---|

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

| Number of earlier application | Date of filing *(day / month/ year)* |
|---|---|

8. Is a statement of inventorship and of right to grant of a patent required in support of this request *(Answer 'Yes' if:*

*a) any applicant named in part 3 is not an inventor, or*
*b) there is an inventor who is not named as an applicant, or*
*c) any named applicant is a corporate body.*
*See note (d))*

NO

**Patents Form 1/77**

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

| | |
|---|---|
| Continuation sheets of this form | 0 |
| Description | 11 |
| Claim(s) | 0 |
| Abstract | 0 |
| Drawing(s) | 3 |

10. If you are also filing any of the following, state how many against each item.

| | |
|---|---|
| Priority documents | - |
| Translation of priority documents | - |
| Statement of inventorship and right to grant of a patent *(Patents Form 7/77)* | - |
| Request for preliminary examination and search *(Patents Form 9/77)* | - |
| Request for substantive examination *(Patents Form 10/77)* | - |
| Any other documents *(please specify)* | - |

11. I/We request the grant of a patent on the basis of this application.

Signature [signature] Date 7 July, 2003

R.G.C. JENKINS & CO

12. Name and daytime telephone number of person to contact in the United Kingdom D. C. Musker 020-7931-7141

**Warning**

*After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.*

**Notes**

*a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

*b) Write your answers in capital letters using black ink or you may type them.*

*c) If there is not enough space for all relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

*d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

*e) Once you have filled in the form you must remember to sign and date it.*

*f) For details of the fee and ways to pay, please contact the Patent Office.*

## Anti-Piracy System

### 1. Prior Art

### 1.1 Flooding of P2P networks with false files

It is well known that music (and other copyright materials) is widely available on the Internet via "file sharing" or "peer-to-peer" ("P2P") systems such as "Napster" and its successors. These have been very difficult to prevent by traditional methods such as litigation. Some companies and artists have uploaded corrupted, incorrectly named or blank files to P2P networks to make it harder for people to find music. The spreading of fake files is commonly known as 'spoofing'. For example, Madonna placed a file onto the P2P networks entitled 'American Life' which was blank, save her shouting: "What the **** do you think you're doing!"

### 2.1 Sending messages via Instant messenger

In a desperate attempt to slow the spread of online music piracy, The Recording Industry RIAA has developed software that enables it to find users swapping unauthorized copies of songs on the Internet and send instant messages that pop up on the their computer screens with a copyright infringement warning.

### 1.3 Problems with prior art

An application called PeerGuardian developed by Tim Leonard, a 23-year-old English programmer, currently blocks more than four million IP addresses, and users can continually update that list. PeerGuard, therefore, renders the process of sending messages or false files to the P2P networks ineffective.

## 2. Interpretation and Definitions

"Peer-to-peer network (P2P)"

On the Internet, peer-to-peer (referred to as P2P) is a type of transient Internet network that allows a group of computer users, with the same networking program, to connect with each other and directly access files from one another's hard drives. Examples of well-known P2P software include Grokster, Morpheus, iMesh and Kazaa.

Once installed, the computer finds another network member on-line, it will connect to that user's connection. Users can choose how many member connections to seek at one time and determine which files they wish to share.

P2P users can search for specific files via a sophisticated key word search. For example, music files can be found by artist name or track title. To ensure the fastest and most reliable connection, the P2P software locates several of the same file from a multitude of different locations. By switching from hard drive to hard drive a single file, made up of small packets of data or segments, could have originated from many different sources.

"STEM server"

The STEM server contains a database which holds a list of STEM protected files and protected material definitions as well as statistical information and updates. The STEM server will also host the website and the PMCS (Protected Material Copyright Panel) which allows IP owners to manage and protected their material externally via a secure website.

"STEM node (also referred to as STEM Agent)"

STEM nodes search for files that are stored on the STEM server database checking against the protected material definitions (i.e. files that are owned by STEM's clients and which need protection). STEM nodes then connect to P2P networks and emulate P2P users but instead of offering genuine files, only files containing false data are made available. STEM nodes are deployed via a STEM screensaver application.

"STEM screensaver"

The STEM screensaver performs several functions but its primary purpose is to connect STEM nodes to P2P networks. It also acts as a communications channel between the STEM server and web users that install the STEM screensaver. The following is a summary of the STEM screensaver's functions:

a) Contains STEM nodes that connect and disrupt P2P networks.

b) Regular STEM server requests to update protected file definitions.

c) Checks for software updates (ensuring the protection system is one step ahead of the P2P networks)

d) Uploads performance data and statistics to the STEM server which monitors the screensaver's performance (statistics show, for example, how long the screensaver has been connected and how many files have been protected etc).

e) Acts as a communications channel between STEM and users who have installed the STEM screensaver on their PC.

By default the screensaver will become active whenever a computer is not being utilised by its owner. The owner can, however, define the STEM screensaver's settings, activating it manually or presetting it to run at specific times.

"STEM protected files"

STEM is capable of targetting specific files that reside on P2P networks whilst ignoring files that have not been targeted for protection.

"PMCS (Protected Material Copyright Panel)"

The PMCS can be accessed via a password protected web-based interface and is a database (located on the STEM server) containing a list of files that clients have paid STEM to protect. The PMCS will also allow companies to update their protected material definitions automatically, as well as add new protected material.

"File segment"

Once a file has been introduced to a P2P network (transferred onto the hard drive of a member's PC) it can then be duplicated and saved onto the hard drives of hundreds, thousands or even millions of P2P members' hard drives. To speed up the download/sharing process small 'segments' of the same file can be downloaded from many different users' hard drivers simultaneously.

"Client"

The person or corporate entity that has paid STEM a fee to prevent their intellectual property from being duplicated via P2P networks.

"Loyalty Scheme"

A scheme that encourages internet users to install the STEM screensaver onto their computers. Loyalty incentives include, although not exclusively, discounts, entry to competitions or other forms of monetary consideration. The level of compensation could be linked to the amount of time the STEM node/screensaver has been active.

"Bandwidth"

The amount of information that can be transfered in a given time period (usually a second) over a wired or wireless communications link.

"Maximum Allowed Connections"

P2P software limits the amount of single user simultaneous connections. This is usually set at 50 meaning that only 50 users can be downloading information at any one time.

"Protocols and Parameters"

Each P2P network uses a unique set of protocols and parameters. For example, the way in which each P2P network shares and searches for information differs. Also, the way in which members are rewarded may differ (P2P users who share more files than they take are given higher access privileges than those who take

more files than they share). All these functions are specific to each P2P network and will need to be emulated by the STEM node.

"Update"

Where the server updates the information on the STEM node or vice versa. This maybe but not limited to security updates, protocol and parameter updates, protected material updates and statistical information updates.

"Protected Material"

Any material or intellectual property in digital form that resides on a P2P network, that a client has paid STEM to protect. This could include but not limited to Music Files, Video Files and Software.

"Files"

In any computer system but especially in personal computers, a file is an entity of data available to system users (including the system itself and its application programs) that is capable of being manipulated as an entity (for example, moved

From one file directory to another). The file must have a unique name within its own directory. Some operating systems and applications describe files with given formats by giving them a particular file name suffix. (The file name suffix is also known as a file name extension. For example, a program or executable file is sometimes given or required to have an ".exe" suffix. In general, the suffixes

tend to be as descriptive of the formats as they can within the limits of the number of characters allowed for suffixes by the operating system for example, WAV, MP3, MPEG, EXE, ZIP, CAB, MID and DIVx.

"Protected Material Definitions"

A set of definitions that are used to protect a file. This could be but not limited to a track name, artist name, movie title, associated name search phrase, common miss-spellings associated with the protected material or other relevant information linked to a file.

"STEM Users"

Any person who installs a STEM screensaver containing the STEM node.

"P2P user software"

The software that resides on a P2P user's computer which allows them to connect to a pier to pier network.

"P2P user"

An individual or organisation that utilises P2P software to connect to a P2P network.

"Imitation/decoy Data"

Any data sent across the P2P network that purports to be a whole or part of a file that does not contain the actual data the user requested.

## 2. Simultaneous Technology Emulation Management (STEM) – Description of preferred embodiments

### 2.1 Basic Premise

An embodiment of the invention referred to as STEM is a technology solution designed to prevent "sharing" of copyright protected material over P2P networks. The invention encompasses a computer system comprising a server and one or more client terminals (e.g. PCs running a browser program). It also extends to the software running on the server, and that downloaded to the clients, alone and as a computer program product.

The embodiment achieves this by emulating the way in which P2P user software operates, but instead of connecting genuine P2P users together with genuine data, STEM floods the network with thousands of false connections and false data. When a real P2P user unwittingly logs onto the computer of a 'bogus' P2P user (which is in reality a STEM node), the real P2P user starts to retrieve false data. The way in which this is achieved is covered in more detail under section 3.3 Protection Systems.

Each individual component STEM protection system described in Section 3.3 works well on its own and could be used without the others. However, the combination of protection systems (see Section 3.3 for further details), makes STEM even more potent. Furthermore, the protection systems described in Section 3.3 ensure that each STEM node is capable of monitoring a significant number of P2P users, preventing them from operating effectively. This means that even if far few STEM nodes compared to P2P users are active at any one time, a significant level of protection can still be provided **(See Figure 1)**. The use of a screensaver network to combat piracy is also an independently operable aspect of the invention.

**Advantages of embodiments in overcoming problems with prior art**

'Spoofing' has largely been ineffective because P2P users have become aware that spoof or decoy files tend to download more readily and at higher speeds than 'genuine' files. It is important to note that STEM ensures that when decoy files are distributed via STEM nodes, they display similar characteristic to genuine files i.e. they download erratically and less reliably.

PeerGuardian will be ineffective against STEM as P2P users have variable IP addresses when logging onto P2P networks. Also, the sheer volume of STEM nodes predicted to be in operation will almost certainly overwhelm PeerGuardian's identification and blocking system.

## 3. STEM – Detailed technical/functional description

### 3.1 Detailed functionality description

STEM works by flooding the P2P user's connection with bogus data making it more difficult for other P2P users to download the same data. This is important as only data that has been selected for protection by the STEM system is affected in this way. Non STEM-protected material is unaffected. It also utilises other features of P2P networks to corrupt or interrupt the distribution of protected material.

The STEM solution works by utilising the power of distributed computer technology via a series of STEM nodes that are deployed from STEM screensaver software allowing STEM nodes to work together in a collaborative manner, making protected material on P2P networks unobtainable. The solution still allows P2P networks to distribute/share material that is not protected by STEM.

files from P2P networks they will often monitor the speed at which the file is being downloaded. If the connection speed is too slow the P2P user will normally cancel the file download session and find a faster one. To avoid this from happening, the STEM node allows the file to download at an acceptable speed initially but gradually reduces the amount of bandwidth substantially slowing the file transfer rate. The reason for this is twofold. Firstly, it is STEM's aim to inconvenience P2P users without inconveniencing those that have installed the STEM screensaver. By reducing bandwidth levels to a minimum, users who have chosen to install the STEM screensavers will not notice that their bandwidth is being used to carry out the STEMMING system process (i.e. the transfer of small amounts of bogus data to P2P users hard drives). See figure 3.

c) Segment of the file interruption

When a P2P user downloads a file, the P2P network software automatically seeks out multiple P2P users to download the file from to speed up the download process. The STEM node will be able offer a segment of that file to a user, when the P2P software starts to download the segment from our STEM node we will be sending imitation data. This imitation data when combined with the whole file will render the whole file corrupted (**See figure 4).**

d) P2P connections overload

Every P2P user software has a maximum number of connections parameter, this limits the number of computers that can download from that user at any one time. By leveraging the benefits of distributed computing the STEM nodes can create multiple connection to a P2P user that has illegal information on their computer. Once this has reached the maximum number of connections for that P2P user it will be impossible for any other user's to download from that P2P user. This has the benefit of requiring very little bandwidth as the STEM node can have multiple connections running at the very minimum bandwidth (**See figure 5).**

3.4 Data Acquisition

STEM nodes actively seek out protected material that is contained on the hard drives of P2P users; checking the contents against the protected material definitions. When protected material is found the STEM node connects to the STEM server which in turn communicates with other STEM nodes. At this point

STEM nodes respond by activating the aforementioned protection systems as described in item 3.3 of this document. This response is similar to a denial of service attack on the internet.

Mutual identification system

The mutual identification system prevents STEM nodes from seeking out protected material residing on other STEM nodes (i.e. making sure that STEM nodes can tell the difference between decoy files and real files). Without the mutual identification system a feedback loop would occur where STEM nodes would start 'attacking' other STEM nodes.

Mutual Amplification System

Some P2P networks use ratings to judge how reliable and fast a P2P user's connection is and how many files they share and take. The Mutual amplification system allows STEM nodes to mutually share files (of a small nature) to increase their rating within the P2P network.

STEM node network functionality

Combining the bandwidth and processing power of many STEM nodes is similar to distributed computing but what makes the system unique is the way in which it interfaces with the server, the Data Acquisition Protection System, mutual verification system, and mutual amplification system.

STEM data acquisition

When a client sets up a Protected Material Definition the STEM data acquisition system will then search for files on the P2P network that match the definitions. When it has found a file that matches a definition it will upload the file parameter information such as size and name to the STEM database. It will continually do

this to update the database containing the available files that breach the STEM Protected Material Definition. It will use this information to provide realistic information on available file sizes to the STEM nodes. This will allow the STEM nodes to provide realistic information on the files so that you cannot tell if it is a real file or an imitation/decoy file. This is also critically important for the file segment interruption as the file size must be exactly the same as the real file or the P2P user software will reject it.

**Modifications and Variants**

Protection is hereby sought for any and all novel subject-matter and combinations thereof disclosed herein.

The present invention extends to any and all variants to the above-described techniques that would be obvious to the skilled person.

**Fig. 1**

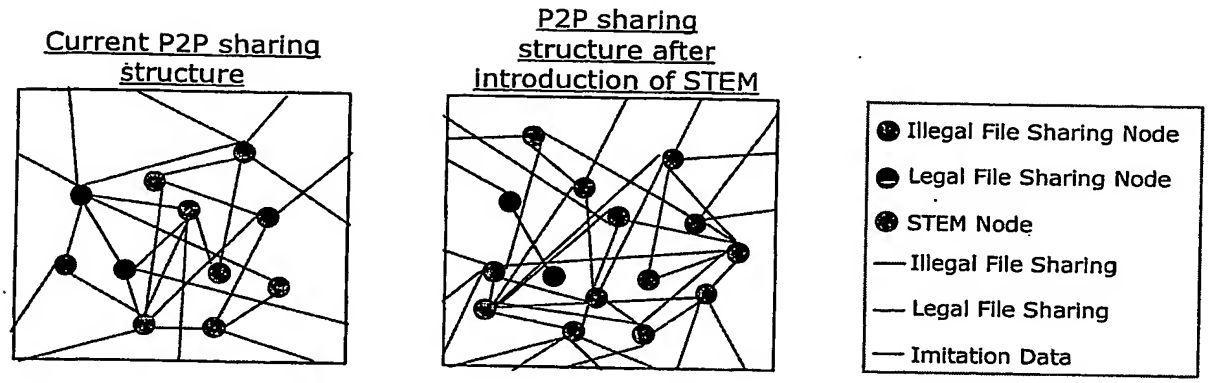

Current P2P sharing structure
P2P sharing structure after introduction of STEM
Illegal File Sharing Node
Legal File Sharing Node
STEM Node
Illegal File Sharing
Legal File Sharing
Imitation Data

**Fig. 2**

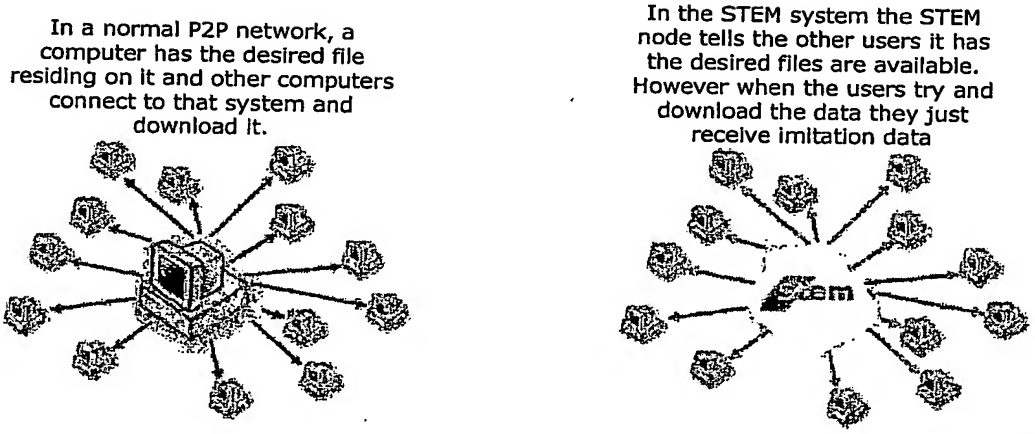

In a normal P2P network, a computer has the desired file residing on it and other computers connect to that system and download it.
In the STEM system the STEM node tells the other users it has the desired files are available. However when the users try and download the data they just receive imitation data
Stem

**Fig. 3**

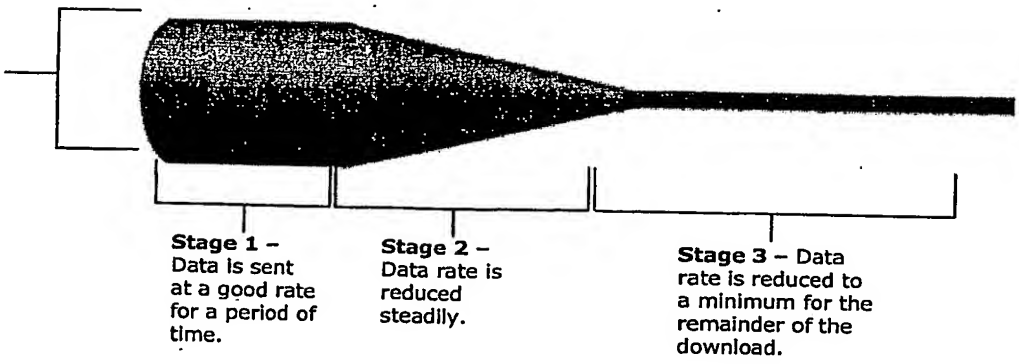

Stage 1 – Data is sent at a good rate for a period of time.
Stage 2 – Data rate is reduced steadily.
Stage 3 – Data rate is reduced to a minimum for the remainder of the download.

**Fig. 4**

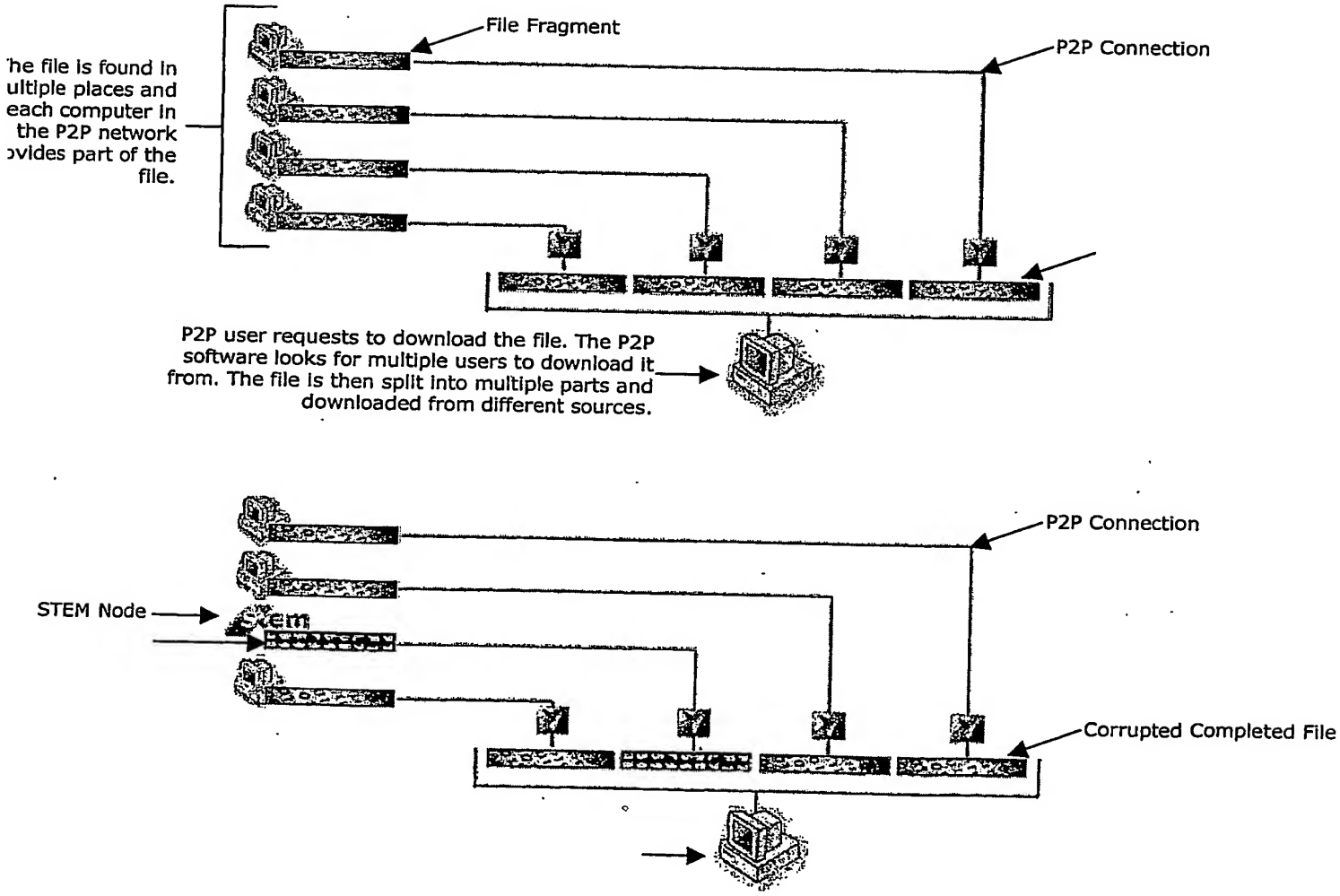
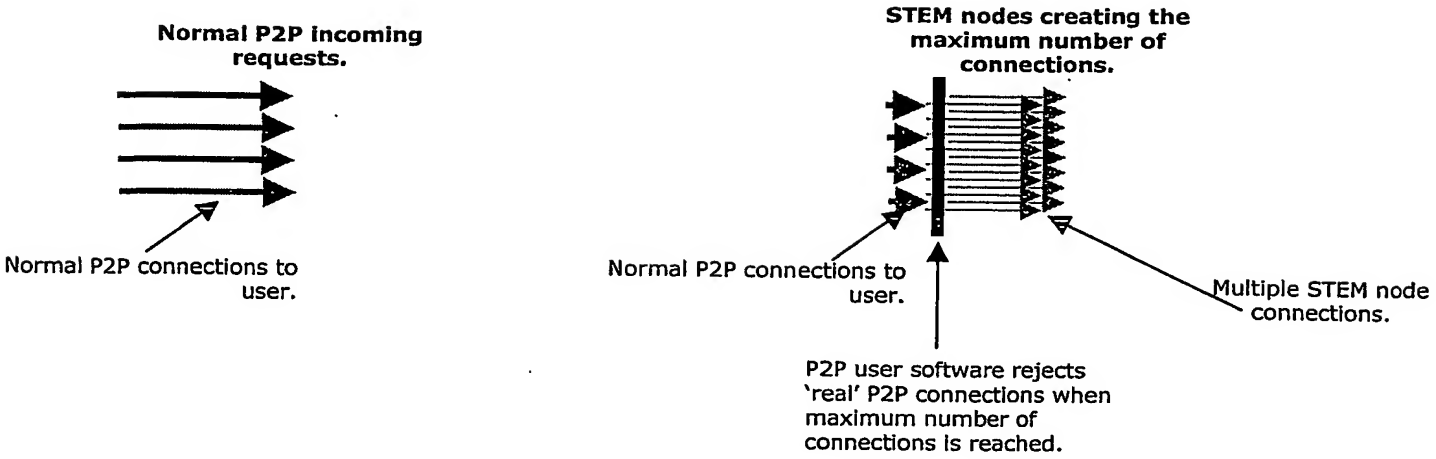

he file is found in ultiple places and each computer in the P2P network ovides part of the file.
File Fragment
P2P Connection
P2P user requests to download the file. The P2P software looks for multiple users to download it from. The file is then split into multiple parts and downloaded from different sources.
P2P Connection
STEM Node
Corrupted Completed File

**Fig. 5**


Normal P2P incoming requests.
Normal P2P connections to user.
STEM nodes creating the maximum number of connections.
Normal P2P connections to user.
Multiple STEM node connections.
P2P user software rejects 'real' P2P connections when maximum number of connections is reached.